REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application. Applicant would also like to thank the Examiner for correctly indicating as allowable the subject matter of dependent Claims 3, 5, 6, 8, 11, 13, 15-16, 19, 21-24, 27-28 and 33-34. The arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 1, for example, is directed to a method for securing circulation of an encrypted digital document to be reproduced with a document reader. The method comprises providing a user with a storage device storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated with the storage device.

The method further comprises transmitting to a server over a digital data transmission network from the storage device to the server upon connection of the storage device to the server by a terminal connected to the digital data transmission network and to the storage device information identifying the digital document to be reproduced, and the information list and the identification information of the storage device.

The method further comprises identifying from the server the storage device on the basis of the information identification of the storage device transmitted to the server. Possible fraudulent use of the storage device is determined based

upon the information list that is transmitted to the server. The server compares the identification information in the information list with an authorized or fraudulent reader list for determining fraudulent use of the storage device. If the storage device is not being fraudulently used, then the method comprises transmitting over the digital data transmission network from the server to the computer terminal a decryption key specific to the digital document to be reproduced, with the decryption key being stored in the storage device. The digital document is decrypted using the stored decryption key by the document reader connected to the storage device. The digital document decrypted by the document reader is reproduced.

Independent Claim 9 is also directed to a method for securing circulation of an encrypted digital document to be reproduced with a document reader, and is similar to independent Claim 1.

Independent Claim 17 is directed to a system for securing circulation of an encrypted digital document to be reproduced with a document reader, and is similar to independent Claim 1.

Independent Claim 25 is also directed to a system for securing circulation of an encrypted digital document to be reproduced with a document reader, and is similar to independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 9, 17 and 25 over the Cheah et al. patent in view of the Chatani et al.

patent. The Examiner cited Cheah et al. as disclosing the claimed invention except for transmitting information identification to a server over the digital data transmission network from the storage device to the server upon connection of the storage device to the server by a terminal connected to the digital data transmission network and to the storage device; and identifying from the server the storage device on the basis of the information identification of the storage device transmitted to the server.

The Examiner referenced Chatani et al. as disclosing that server and computer systems transmit and receive data over a computer network or standard telephone line. The Examiner also noted that Cheah et al. and Chatani et al. are analogous art because both teach securing distribution of encoded digital data/digital documents.

The Examiner has taken the position that it would have been obvious at the time of the invention to modify Cheah et al. to include server and client computer systems that transmit and receive data over a computer network as in Chatani et al. because identification information is transmitted by the user to the server to generate the unlock key used by the user for further interpretation.

The Applicants submit that even if the references were selectively combined as suggested, the claimed invention is still not produced. First, Cheah et al. fails to disclose a storage device storing identification information of recent readers previously used with the storage device. Reference is directed to column 4, lines 40-59 of Cheah et al., which provides:

> "After insertion of memory card **32** into memory card port **38** of audio player **10** and prior to beginning playback, micro-controller **22** reads memory card **32**, in particular a configuration file stored therein, to identify and display the audio data files stored on memory card **32**, and their associated encoding formats. When the user selects a particular audio data file for playback, micro-controller **22** loads the selected audio data file and the appropriate decoder file into DSP RAM **11**, wherein DSP **12** decrypts both the data and decoder files, and then decodes the selected audio data file using the decoder file. Thus, the decoder files on memory card **32** allow audio player **10** to be adapted to process the various encoding formats associated with the audio data files stored on memory card **32**. In effect, portable audio player **10** is software upgraded, as necessary, by the decoder files stored on memory card **32** when the user selects a particular audio data file stored on memory card **32**. The steps associated with processing a selected audio data file from memory card **32** using audio player **10** is shown in the flowcharts of FIGS. 3 and 4, and described below."

The above reference cited by the Examiner merely discloses an audio player which reads a configuration file in a storage device to identify audio data files stored therein. After selection by the user of an audio file, the reader loads from the storage device the selected audio file and an associated decoder file. Then the reader decrypts the loaded audio and decoder files, and decodes the audio file using the decoder file.

Reference is also directed to column 6, lines 34-55 of Cheah et al., which provides:

> "In the present invention, audio data files are loaded onto memory card **32** using music management software that encodes the audio data files in accordance with a selected encoding format, such as MP3, encrypts the encoded data files, and then stores the encrypted, encoded data files. Various encryption and decryption methods known to those skilled in the art for generating an encrypted file using a selected key, and then decrypting the encrypted file using the selected key may be used. In the present invention, the decoder files are encrypted using a first key, and the audio data files are encrypted using another key that is generated using the unique identifier on memory card **32**. The music management software stores the encrypted audio data files and appropriate encrypted decoder files onto memory card **32**. The music management software also generates, and modifies as necessary, a configuration file and a file attribute table to provide information regarding the various data files and decoder files stored on memory card **32**. Using the configuration file and the file attributes table, audio player **10** is able to determine the correct encoding format for each content file, display the available file on display **21** and download appropriate decoder file for each content file in response to a user selection."

The above reference cited by the Examiner merely discloses a memory card (i.e., storage device) which memorizes encrypted and encoded audio files and encrypted decoder files.

The decoder files are encrypted using a first key, and the encoded audio files are encrypted used a second key that is generated from an identifier of the memory card. This paragraph also discloses a configuration file and a file attribute table providing information about the audio files and decoder files that are stored on the memory card.

Cheah et al. further fails to disclose determination of a fraudulent use of the storage device if the list of the last readers used with the storage device contains an identifier of an unauthorized or fraudulent reader. For this feature of the claimed invention, the Examiner referenced column 1, lines 51-63 of Cheah et al., which provides:

> "Unauthorized copying and distribution of digitally encoded data is a significant concern associated with such players, especially in light of the growing popularity of such devices and the relative ease with which such data is downloaded and distributed over the Internet and other sources. Therefore, it is desirable to provide a portable audio data processing apparatus and a method for processing encoded audio data prevents a user from playing data that has been copied without authorization. Also, it is desirable to prevent a user from making multiple playable copies of an audio data files from one removable data storage device, such as a compactflash™ memory card, to a similar type of data storage device."

However, the above paragraph merely discloses how to prevent a user from playing an audio file that has been copied

from another storage device (without authorization), and to prevent a user from making copies of an audio file stored in a storage device to a similar storage device. Since Cheah et al. fails to disclose a list of identifiers of the last readers used with a portable or removable storage device, Cheah et al. thus fails to disclose determining a fraudulent use of the storage device from such a list.

Moreover, Cheah et al. fails to disclose a server for exchanging data with the storage device. Consequently, Cheah et al. fails to disclose transmission of the identifier of the storage device with the list of identifiers of the last readers used with the storage device, as in the claimed invention. Only the reader of Cheah et al. can determine a fraudulent use of the storage device if decryption of an audio file fails due to the fact that the decryption key is wrong, and this determination is not performed using a list of reader identifiers.

The Chatani et al. application is directed to a computer network system for securely distributing computer software products, and fails to provide the noted deficiencies of Cheah et al. FIG. 1 in Chatani et al. illustrates a block diagram of the computer network system. More particularly, Chatani et al. is directed to a product distribution and payment system for limited use or otherwise restricted digital software products. Digital content data comprising a software product to be rented is made available to customers through a detachable local storage medium, such as a DVD or CD-ROM disc, or over a network connection.

The product digital content is capable of being

accessed and played back through a computer or game console at the customer's site. The software product may comprise a limited use product that is restricted in the number of plays or duration of use. The customer is allowed to download and purchase the product using his computer or playback console. The product purchase information is encoded and transmitted to the content distributor. When the preset time or number of plays has elapsed the software program is frozen and access to the program is not allowed.

As compared to the claimed invention, the Applicant submits that Chatani et al. discloses a completely different approach for determining possible fraudulent use of the storage device. Fraudulent use of the storage device in Chatani et al. is based on the software product being a limited use product. When the software product is purchased, the buyer selects the desired type of limited use product. Reference is directed to paragraph 45 in Chatani et al., which provides:

> "... In step **322**, the user follows the instructions of the server to select the purchase option he or she prefers. For a limited use product, the user may be prompted to select between renting the product for a certain period of time or for a certain number of accesses (game plays), or combinations thereof. ..." (Emphasis added).

The Applicant submits that Chatani et al. fails to disclose that a possible fraudulent use of the storage device is determined based upon an information list that is transmitted to

the server, as in the claimed invention. In the claimed invention, the information list comprises identification information identifying recent document readers previously operated with the storage device, and the server compares the identification information in the information list with an authorized reader list for determining fraudulent use of the storage device.

In Chatani et al., the Examiner references paragraph 60 which discloses that when the user makes a purchase, a database record is maintained which records both the serial number of the playback machine and the serial number of the disk. If the user is ever forced to replace their playback machine, he or she could request a new unlock key by inserting the disk into the new playback machine. The database then confirms that the disk serial number shows a purchase against it, and therefore allows a new unlock key to be generated for the user.

The Applicant submits that by keeping track of the disk serial number which shows a purchase against it, there is no need to compare the identification information (i.e., recent document readers previously operated with the storage device) in the information list with an authorized reader list for determining fraudulent use of the storage device. Instead of focusing on an authorized or unauthorized reader list in Chatani et al., Chatani et al. focuses on when the preset time or number of plays has elapsed for the purchased software program. Once one or both of these parameters has elapsed, then the software program is frozen and access to the program is not allowed. The database in Chantani et al. simply confirms that a purchase has been made

with respect to the disk via its disk serial number.

In sharp contrast, possible fraudulent use of the storage device in the claimed invention is based upon the information list that is transmitted to the server, and the server compares the identification information in the information list with an authorized reader list for determining fraudulent use of the storage device. In Chatani et al., replacing the playback machine with a new playback machine has nothing to do with an authorized or unauthorized reader list of recent document readers previously operated. Chatani et al. merely teaches the use of a database recording, for each disk purchased, the serial number of a single playback machine and the serial number of the purchased disk and the generation of the decryption key on the basis of the serial numbers.

Accordingly, it is submitted that independent Claim 1 is patentable over Cheah et al. in view of Chatani et al. Independent Claims 9, 17 and 25 are similar to independent Claim 1. Therefore, it is submitted that these claims are also patentable over Cheah et al. in view of Chatani et al.

In view of the patentability of independent Claims 1, 9, 17 and 25, it is submitted that the other rejected dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a

In re Patent Application of:
KASSER
Serial No. **10/799,371**
Filed: **MARCH 13, 2004**

Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330